UNITED STATES DISTRICT COURT

for the

Eastern District of California

United States of America
v.

BRADLEY ALLEN GREENWOOD

Defendant(s)

Case No. 2:25-mj-0075 JDP

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of November 16, 2021 in the county of San Joaquin in the Eastern District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 2252(a)(2)	Receipt/Distribution of Child Pornography

This criminal complaint is based on these facts:

(see attachment)

☒ Continued on the attached sheet.

/s/ Kevin Kandow
Complainant's signature

Kevin Kandow, Special Agent, FBI
Printed name and title

Sworn to me and signed via telephone.

Date: April 30, 2025

Judge's signature

City and state: Sacramento, California

Jeremy D. Peterson, U.S. Magistrate Judge
Printed name and title

AFFADAVIT

I, Kevin Kandow, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a criminal complaint and arrest warrant under Federal Rule of Criminal Procedure 4.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since March 1, 2020. I attended over 20 weeks of training at the FBI Academy in Quantico, Virginia and received training in areas including criminal investigations and constitutional law. I have planned and executed multiple federal search warrants. I have been assigned to the Stockton Safe Streets Task Force conducting investigations of narcotics, firearms, gang violence, and crimes against children.

3. As a Special Agent with the FBI, I have received training in the investigation and prosecution of violations of various federal laws, including those related to child pornography and child exploitation. I have received specialized training regarding crimes against children matters. I have interviewed multiple victims and witnesses for investigations involving child sexual exploitation, child pornography, and other crimes against children. I have observed and reviewed thousands of examples of sexually explicit conduct involving minors and child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media such as smart phones. As a federal agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 2422, 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant, and therefore, does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that BRADLEY ALLAN GREENWOOD (hereafter "GREENWOOD") violated 18 U.S.C. § 2252(a)(2) (Receipt and/or Distribution of Child Pornography). This affidavit

therefore supports my application for an arrest warrant for GREENWOOD for these offenses.

III. BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

6. Law enforcement agents have been investigating child pornography trafficking by users of "Freenet" — an Internet-based, peer-to-peer (P2P) network that allows users to semi-anonymously share files, chat on message boards, and access websites within the network — since 2011. Law enforcement linked a Freenet user in Lodi, CA, later identified as GREENWOOD, to the sharing and trafficking of child pornography.

Background Regarding Freenet

7. In order to access Freenet, a user must first download the free and publicly available Freenet software. The Freenet "source code" — i.e., the computer programming code that facilitates Freenet's operation – is also publicly available. In other words, Freenet is "open source" software that may be examined and analyzed by anyone with the pertinent expertise or knowledge.

8. Anyone running the Freenet software may join and access the Freenet network. Each computer running Freenet connects directly to other computers running Freenet, which are called "peers."[1] When installing Freenet, each user agrees to provide to the network a portion of the storage space on the user's computer hard drive, so that files uploaded by Freenet users can be distributed and stored across the network. Freenet users can upload files into the Freenet network and download files from the Freenet network. After a user installs Freenet on the user's computer, the software creates a default "download" folder. If a user successfully downloads a particular file from Freenet, Freenet may save the content of that file to the "download" folder. A user may change this default setting and direct the content to be downloaded elsewhere.

9. When a user uploads a file into Freenet, the software breaks the file into pieces (called "blocks") and encrypts each piece. The encrypted pieces of the file are then distributed randomly and stored throughout the Freenet network of peers.[2] The software also creates an index piece that contains a list of all of the pieces of the file and a unique key – a series of letters, numbers and special characters

[1] The number of peers is determined by the user's settings and is based on the quality and speed of the user's Internet connection.

[2] Because the pieces of files are encrypted, a Freenet user is unable to access the content of pieces that are stored on the user's computer hard drive, which are not in a readable format.

– that is used to download the file.

10. In order to download a file on Freenet, a user must have the key for the file. There are several ways that a Freenet user can download a file using a key. Some examples include: (1) the "download" box on Freenet's "file sharing" page; (2) the "download" box on the message board associated with Freenet or other Freenet add-on programs; and (3) directly through the user's web browser while the user is connected to the Freenet network.

11. When a user attempts to download a file via Freenet, Freenet downloads the piece of the file containing the index, which provides the information required to retrieve the individual pieces of the file. The Freenet software then requests all of the pieces of the file from the user's peers. Rather than request all of the file pieces from a single peer, requests for file pieces are divided up in roughly equal amounts among the user's peers. If a user's peer does not have the particular requested pieces in its storage, that peer will then divide up and ask its peers for the pieces, and so on. For example, if User "A" has 10 peers and requests 1000 pieces of a file, roughly 100 pieces are requested from each one of User A's peers. See Figure 1.

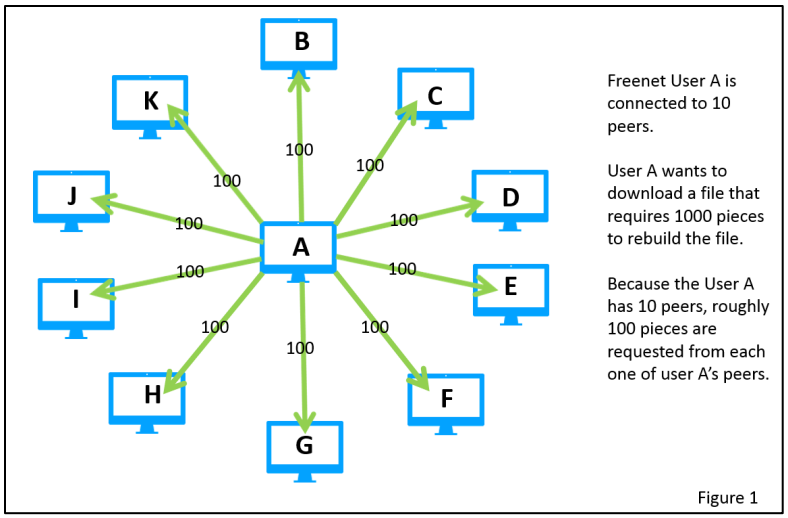

Figure 1

If Peer "B" receives User A's request for 100 pieces of the file, but does not have any of those pieces in its storage, Peer B forwards on the request for those pieces to Peer B's peers. If Peer B has 10 peers of its own, roughly 10 pieces are requested from each one of Peer B's peers. See Figure 2.

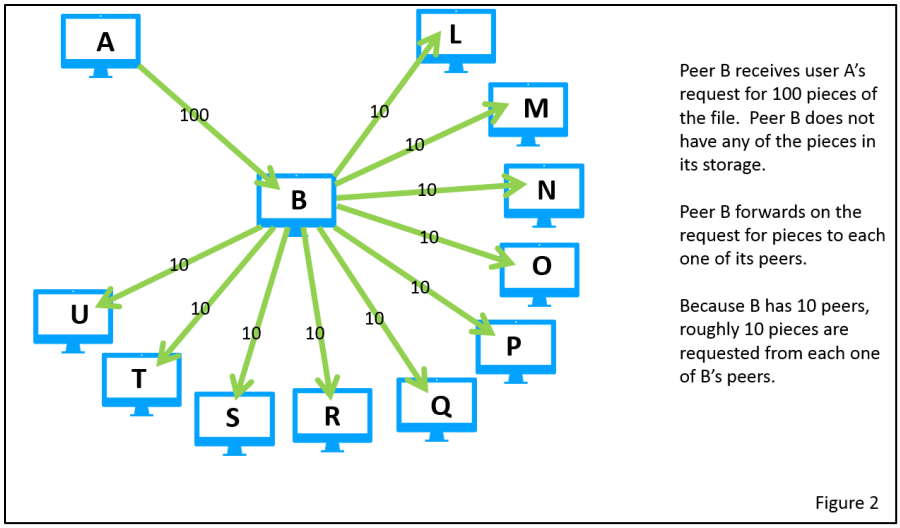

Figure 2

This design can help distinguish between a Freenet user that is the original requestor of a file, and one that is merely forwarding the request of another user.

12. To prevent requests for pieces from going on indefinitely, Freenet is configured to only allow a request for a piece of a file to be forwarded to another peer a limited number of times (the default maximum is 18). If a request reaches that limit without finding the requested piece, a signal is returned to the user's computer and the request is sent to another of the user's peers. The remaining number of times a request for a piece may be forwarded is included within the request for that piece.

13. Freenet warns its users in multiple ways that it does not guarantee anonymity: when Freenet software is initially installed; within the log file each time Freenet is started; and via Freenet's publicly accessible website. Freenet software also does not mask a computer's IP address. Freenet also acknowledges on its publicly accessible website that, for users who use the Opennet mode, it can be statistically shown that a particular user more likely than not requested a file (as opposed to having merely forwarded the request of another peer) based on factors including the proportion of the pieces of a file requested by a user and the number of nearby peers.

Child Pornography Images/Videos on "Freenet"

14. Freenet can be used to advertise and distribute images and videos of child pornography. Unlike other file sharing systems, Freenet does not provide a search function for its users whereby users would insert search terms to locate files. Therefore, a user who wishes to locate and download child

pornography from Freenet must identify the key associated with a particular child pornography file and then use that key to download the file.

15. Freenet users can identify those keys in a number of ways. For example, "message boards" exist on Freenet that allow users to post messages and engage in online discussions involving the sexual exploitation of minors. Law enforcement agents have observed message boards labeled: "pthc," "boy porn," "hussy," "pedomom," "kidfetish," "toddler_cp," "hurtcore," and "tor-childporn." Typical posts to those message boards contain text, Freenet keys for child pornography files, and in some cases descriptions of the image or video file associated with those keys. Freenet users can also obtain keys of child pornography images or videos from websites that operate within Freenet called "Freesites." Freesites can only be accessed through Freenet. Some of those sites contain images of child pornography the user can view along with keys for child pornography files.

Requests Targeted in the Instant Investigation

16. An FBI Special Agent reviewed information obtained and logged by law enforcement Freenet computers that showed that a Freenet user with IP address 73.235.60.254 requested pieces of the child pornography files described below from a law enforcement Freenet computer. With respect to each file – considering the number of requested file pieces, the total number of file pieces required to assemble the file, and the number of peers the user had – the number of requests for file pieces is significantly more than one would expect to see if the user of IP address 73.235.60.254 were merely routing the request of another user. As a result, the special agent concluded that the user of IP address 73.235.60.254 was the original requestor of each of the described files.

17. On August 9, 2021, agents first detected a computer running Freenet software with an IP address of 73.235.60.254, requesting blocks of suspected child pornography. Law enforcement detected these blocks were requested on or around July 2, 2021. The files were reviewed by law enforcement and were confirmed to be child pornography.

18. On September 19, 23, and 26, 2021, law enforcement detected a computer running Freenet software with an IP address of 73.235.60.254 requesting pieces of known child pornography files. The keys for each of these files were obtained by law enforcement agents at some point after

2011, either from a Freenet message board or Freesite that contained information related to the sexual exploitation of children, or from a previous investigation. Agents then downloaded the files, verified by hash value, and confirmed that they were in fact child pornography.

Identification of GREENWOOD for the Search Warrant

19. Using publicly available search tools, law enforcement determined that IP address 73.235.60.254 was controlled by Internet Service Provider ("ISP") Comcast Cable. Comcast subscriber information identified the subscriber as:

Subscriber Name: Brad Greenwood

Address: 9 Elderica Way, Lodi, CA 95245

20. FBI law enforcement checks were completed that confirmed that defendant Bradley Allan Greenwood, lived at 9 Elderica Way, Lodi, CA.

Federal Search Warrant, Interview, and Review of Computer Devices Seized from BRADLEY ALLAN GREENWOOD

21. Agents executed a federal search warrant at 9 Elderica Way, Lodi on November 16, 2021. Present at the search warrant was the defendant, Bradley GREENWOOD. During the search, Agents discovered a desktop computer located in an office room. The desktop computer was powered on and unlocked. Agents observed that Freenet appeared to be running on the desktop computer at the time of the search warrant.

22. Agents conducted a *Mirandized* interview with GREENWOOD during the search warrant. During the interview, GREENWOOD told agents that the office room with the desktop computer powered on and unlocked was primarily used by him. Subsequently, GREENWOOD admitted to using Freenet to download large quantities of Internet files. GREENWOOD stated that he noticed in his past downloads that there were videos of child pornography. GREENWOOD told Agents that he told his wife he accidentally downloaded these videos and that because of how many files he downloaded it was a possibility that he would download child pornography. After reviewing the files on the desktop, Agents returned to the interview with GREENWOOD. Agents showed GREENWOOD a screenshot of files that were found on one of the hard drives connected to the desktop that was reviewed. GREENWOOD read aloud one of the files found on the hard drive which read "12yo Sandra likes anal".

GREENWOOD then stated “I can't justify what anything I do.” And then later stated “I don't know, just shoot me.” GREENWOOD later stated, “The Internet gets so bored that you just download stuff that’s forbidden for the hell of it” and then stated “It’s like obsession.” Agents observed a message board open on the desktop computer related to child pornography and how to download child pornographic files. GREENWOOD stated that he was not active in the message board and did not converse with other users nor post anything on the message board. GREENWOOD recognized what the message board was used for. When asked about the Freenet message board where users chat about child pornography and how to download child pornography GREENWOOD stated that “Yeah, I’ve seen em, yeah." When asked if GREENWOOD read other users’ messages on the message board, GREENWOOD stated “It’s possible.” When asked why he was on the message board GREENWOOD stated “I don’t know, I I I uh, when, if I see a deviant conversation sometimes I look in, there’s other stuff too.” And later stated “I’m just curious.” GREENWOOD first downloaded child pornography “As soon as the Internet came around” and later clarified it was sometime in the 1990's. When asked how he first came across child pornography, GREENWOOD stated that he was on AOL and someone sent him a picture. The first time GREENWOOD saw child pornographic material was available as downloadable content was on Usenet/News Groups in the 1990’s. That’s where the “lions share” of the downloads for child pornography came from. GREENWOOD's stated reason for his interest in downloading and viewing child pornography when he first started was because of the "shock value." GREENWOOD stated that the last few years downloading child pornography had lost its "shock value" and his reason for continuing to download child pornography was because it was "very habitual." GREENWOOD had prostate cancer in 2007 and was unable to partake in any sexual activity since then. GREENWOOD stated several times during the interview that his interest in child pornography was not due to sexual reasons. GREENWOOD stated that the last time he downloaded child pornography was about a month ago. GREENWOOD believed that throughout his life he had viewed at least 100 images/videos of child pornography. When asked if GREENWOOD had viewed over 1,000 still images/videos of child pornography GREENWOOD stated that he couldn't say. GREENWOOD admitted that he had viewed child pornography depicting prepubescent children but that his preference was typically pubescent children from age 13 - 17. GREENWOOD stated that the age 13 was when he first felt "attracted" to

girls and that it was normal for men to have attraction to girls of that age. GREENWOOD stated "I will say though, that anyone after puberty, I would find attractive." Throughout the interview GREENWOOD stated that he took responsibility for what was on his computer devices. GREENWOOD recognized that he had thousands of files of child pornography and stated he "knew it was still on the hard drives" in reference to child pornography but that he was "too lazy to get rid of it."

23. Pursuant to the federal search warrant, the computers and external hard drives seized at 9 Elderica Way, Lodi, CA were forensically imaged. In total, there was at least 20TB of data that was forensically imaged. Due to the amount of data storage on the computer devices seized, it took computer forensic personnel several months to image the devices. Due to large amount of data, the review and tagging of relevant files and data took a significant amount of time and resources to complete. After reviewing and analyzing the 20TB of data, Agents found that FBI evidence items 1B9 (Hard drive, S/N: WCC4E7LYVNXP), 1B10 (Hard drive, S/N WMAWZ0383308), 1B11 (Hard drive, S/N: WCC7K1HCTRFZ), and 1B20 (HP Pavilion Desktop Tower S/N: MXX60204VT) had child pornographic material on them.

24. Evidence item 1B9 (Hard drive, S/N: WCC4E7LYVNXP), was an external hard drive. I observed that there were numerous files which depicted child pornography on item 1B9. Specifically, the filepath **[root]_____ Programs & App's\audacity-win-r8af454f-2.1.3-alpha-01-jan17\Languages_____New** led to several folders with files that depicted child pornography. I viewed some of those files to include the following:

File name: Babysitter Abuse g3Yo

Duration: 26 minutes and 2 seconds long

Description: This file was a video that depicted an adult female and female toddler, aged between 2-4 years old. The adult female undresses both herself and the female toddler during the video. The adult female orally copulates the female toddler as the toddler's vagina is exposed to the camera during the video.

File name: Baby_Lexxa_&_Dad_pee.avi

Duration: Still image

Description: This file was a still image which appeared to be a collage of similar images taken from a webcam. The images depict an adult male use his erect penis to sexually penetrate a 0–1-year-old female baby.

25. There were also several other files that appeared to show knowledge of child pornography being present on item 1B9. For example, there was a folder titled "Links" which was filled with approximately eighty-four Internet shortcut links most of which reference child pornography material and downloading utilizing Freenet. There also was a link titled "How to download CP from Freenet". I believe that “CP” is a reference to child pornography.

26. Task Force Officer (TFO) Gary Viegas reviewed evidence item 1B10 (Hard drive, S/N: WMAWZ0383308). TFO Viegas observed that upon the download artifacts, a “Brad Greenwood” user was logged into a Windows computer system, when the user downloaded thousands of image and video files of child pornography via “Freenet” to the “downloads” folder within the C Drive of this computer system that was used to conduct the downloads. After this discovery, TFO Viegas conducted a search for the actual image and video files as they were listed within the download artifacts, and in most cases TFO Viegas located the specific files with the exact same file names on 1B10. TFO Viegas also found that most often, the individual image and video files of child pornography were stored in folders with the same folder names as those listed within the download artifacts. Given these findings, it appeared that the image and video files of child pornography on 1B10, were originally downloaded by “Brad Greenwood,” to the “downloads” folder within the C Drive of a Windows computer system via Freenet, and then manually transferred to 1B10, an external hard drive, or backed up to this location. Based upon the differing creation dates and times of the image and video files depicting child pornography on 1B10, they were transferred to 1B10 on numerous different occasions between January 2013, and March 2021.

27. I observed that there were numerous files which depicted child pornography on item 1B11 (Hard drive, S/N: WCC7K1HCTRFZ), an external hard drive. Specifically, the filepath **[root]___Audio\00 - Procol Harum - A Whiter Shade of Pale - K2HD Remaster** led to several folders with files that depicted child pornography. The earliest files appeared to have a date of 2003 and a most recent date of 2011. I viewed some of those files to include the following:

File Name: t-017-083

Date Modified: 3/19/2010

Description: The file was a still image which depicted a prepubescent female, aged between 5-7 years old, completely nude. The prepubescent female is bent over with her face turned towards the camera. The prepubescent female's vagina and anus are exposed.

File Name: Tara 9yo_28.jpg

Date Modified: 11/17/2004

Description: The file was a still image depicting a prepubescent female, aged 8-10 years old, completely nude and laying on a bed. The prepubescent female's legs are spread in a position that makes her vagina visible. The prepubescent female has a finger placed inside her vagina. The still image has captioned time stamp 11.17.2004 02:40 on it.

APRIL 30, 2025 SEARCH WARRANT

28. On April 30, 2025, the Hi-Tech Task Force conducted a state search warrant at 19712 Bush Street, Lodi, CA. GREENWOOD was at home during the execution of the search warrant. Your affiant was also present at this search warrant, observed GREENWOOD and identified him as the same GREENWOOD referenced above.

29. During the April 30, 2025, state search warrant at 19712 Bush St, Lodi, CA law enforcement found a computer located in an upstairs office room. The computer was turned on and unlocked. Law enforcement personnel found open Freenet software running and downloading files. Law enforcement observed on the computer that it was BitLocker encrypted, meaning if the computer was turned off someone would need to have access to the BitLocker Access/Recovery Key to un-encrypt the computer. Law enforcement ran a command prompt on the computer and located the recovery key. Subsequently, law enforcement used forensic software to preview the computer and identified known CSAM on GREENWOOD's computer. Your affiant observed law enforcement officers click on some of the known CSAM files identified by the software, and observed several visual depictions of pre-pubescent children completely nude and being sexually abused.

30. A *Mirandized* interview was conducted with GREENWOOD. GREENWOOD admitted to knowingly using Freenet for the purposes of downloading CSAM and returned to downloading

CSAM sometime after the federal search warrant on November 16, 2021. GREENWOOD admitted to viewing CSAM of pre-pubescent children. GREENWOOD admitted to having a sexual attraction to girls as young as 11 years old and above. When asked about the term "PTHC", GREENWOOD responded that he knew what it meant and stated that it meant "Pre-Teen Hard Core".

IV. CONCLUSION

31. In conclusion, I believe that GREENWOOD knowingly received child pornography utilizing the Internet and Freenet. Specifically: GREENWOOD's assigned IP address was found to have been downloading and requesting child pornography utilizing Freenet; during a federal search warrant GREENWOOD's desktop computer was utilizing Freenet and Agents observed file names that suggested the files were child pornographic photos and videos; during a *Mirandized* interview GREENWOOD admitted to knowingly downloading, viewing, and still possessing child pornographic material; and agents located hundreds of thousands of child pornographic images on computer devices/hard drives seized from GREENWOOD. Based on my training, experience, and the information

The remainder of this page intentionally left blank.

contained within this Affidavit, I believe that probable cause exists that GREENWOOD violated 18 U.S.C. § 2252(a)(2) (receipt and/or distribution, of child pornography).

I swear, under penalty of perjury, that the foregoing information is true and correct, to the best of my knowledge, information, and belief.

/s/ Kevin Kandow
Kevin Kandow
Special Agent
Federal Bureau of Investigation

Sworn to before me by telephone and signed by me under authority of Federal Rules of Criminal Procedure 4.1 and 4(d) on April 30, 2025.

The Honorable Jeremy D. Peterson
United States Magistrate Judge

Reviewed and approved as to form

/s/ ROGER YANG
Roger Yang
Assistant U.S. Attorney

United States v. Bradley Allan Greenwood
Penalties for Criminal Complaint

Defendant

COUNT 1: **BRADLEY ALLAN GREENWOOD**

VIOLATION:	18 U.S.C. § 2252(a)(2) - Receipt of Child Pornography
PENALTIES:	Maximum of up to 20 years in prison; or Fine of up to $250,000; or both fine and imprisonment. Mandatory minimum of 5 years in prison. Supervised release of at least 5 years up to life
SPECIAL ASSESSMENT:	$100 (mandatory on each count); $5,000 JVTA / § 3014 (mandatory if the defendant is not found to be indigent); $35,000 if defendant is not found to be indigent.